

Comparison Table/ Methods of Attack

Overall concept / Denial of Service & Brute Force Attacks			
Denial of Service		Brute Force Attacks	
<ol style="list-style-type: none"> <li>1. Shut down the normal operations of a network</li> <li>2. Disrupt the functions of an organization</li> </ol>		3. Like Characteristics	
<ol style="list-style-type: none"> <li>4. Flood a system or network with traffic to prevent legitimate network traffic from flowing</li> <li>5. Disrupt connections between a client and server to prevent access to a service</li> </ol>		<ol style="list-style-type: none"> <li>6. saturate and overwhelm network links with useless data.</li> <li>7. operates on a much larger scale than DoS attacks</li> </ol>	8. Unlike Characteristics
SYN (synchronous) flooding	Ping of death	<ol style="list-style-type: none"> <li>9. the systems that are infected with the DDoS code attack the target site when invoked.</li> </ol>	10. Types
<ol style="list-style-type: none"> <li>11. Sent packets containing invalid source IP addresses.</li> <li>12. Server becomes occupied trying to respond these fake requests</li> </ol>	<ol style="list-style-type: none"> <li>13. A packet that is greater in size than the maximum allowed by IP (65,535 bytes) is sent to a device.</li> <li>14. Cause the receiving system to crash.</li> </ol>	<ol style="list-style-type: none"> <li>1. a fast computer is used to try to guess passwords or to decipher an encryption code.</li> <li>2. tries a large number of possibilities in rapid succession to gain access or crack the code.</li> <li>3. cause a denial of service due to excessive traffic to a specific resource or by locking out user accounts</li> </ol>	
Summary			